# Tema: Sensor-based Mobile Web Fingerprinting and Cross-site Input Inference Attacks

## Síntesis:

Hoy en día la mayor parte de la población cuenta con un dispositivo móvil inteligente, y es inminente que en años futuros aumente más esto, sin embargo, no toda la población que cuenta con un teléfono inteligente sabe de las vulnerabilidades de este, más aún el riesgo de ser víctima de un ataque cibernético ante el uso de alguna aplicación o el uso de la navegación web, en este artículo nos han expuesto alguna de las vulnerabilidades que podríamos presentar con el uso de estos dispositivos.

Hay que tener en cuenta que cualquier dispositivo cuenta con algún sensor, y los teléfonos móviles no son la excepción, estos cuentan con una gran variedad de sensores, en los que destacan la agrupación de los sensores de movimiento, no obstante, se puede acceder a los datos del sensor de movimiento mediante aplicaciones y mediante código JavaScript en páginas web sin que los usuarios de teléfonos inteligentes tengan que otorgar ningún permiso especial porque tradicionalmente **no se consideran confidenciales**. Sin embargo, los ataques avanzados pueden explotar estos datos de sensores de movimiento no sensibles para comprometer la seguridad y privacidad de los usuarios de la web móvil.

En el artículo se mencionan 4 diferentes tipos de ataques, como lo son:

* huellas dactilares de usuarios primeros
* huellas dactilares de usuarios terceros
* interferencia de entrada entre sitios padre a hijos
* interferencia de entrada entre sitios hijos a padre.

En los **ataques de huellas dactilares** de usuario pueden comprometer directamente la privacidad del usuario, ya que esto puede ser usado por el atacante para acceder a sitios web de terceros obteniendo más información sobre la víctima.

Por otro lado, tenemos a los **ataques de interferencia de entrada entre sitios**, en los cuales los atacantes se enfocan en comprometer la seguridad del usuario, el atacante trata inferir en las cuentas del usuario, exponiendo así la seguridad de este.

Ante estos ataques, es importante diseñar mecanismos de defensa de grano fino que puedan ser más utilizables y efectivos en la práctica. Un mecanismo potencial es control de acceso a datos de sensores basado en elementos. Esto también conlleva a tener buenas prácticas de usuario, como el navegar por sitios seguros, al utilizar aplicaciones de confianza, al no introducir datos confidenciales en páginas inseguras, entre otras cosas.

Referencia: Chuan Y., EECS Dept, Colorado School of Mines, IEE Security and Privacy Workshops, 2016, pp. 241 – 244